View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Seton Hall University Libraries

Seton Hall University
eRepository @ Seton Hall

Law School Student Scholarship | Seton Hall Law

2017

Show Me Exactly What You Found: The Private Search Doctrine, Riley v. California and Digital Data

Joshua Koodray

Follow this and additional works at: https://scholarship.shu.edu/student_scholarship

 Part of the Law Commons

Recommended Citation

Koodray, Joshua, "Show Me Exactly What You Found: The Private Search Doctrine, Riley v. California and Digital Data" (2017). *Law School Student Scholarship*. 927.
https://scholarship.shu.edu/student_scholarship/927

Show Me *Exactly* What You Found: The Private Search Doctrine, *Riley v. California*, and Digital Data

Joshua Koodray

Introduction

Men have become the tools of their tools.
- Henry David Thoreau

Henry David Thoreau could not have - or cared to for that matter- imagined the advancements in technology made since his death in 1862.[1] Today, digital technology permeates every aspect of our daily lives. As a society, we have become dependent on our electronic devices and it seems that life, as we know it would cease without them.[2] According to the Pew Research Center, as of January 2014 90% of American adults own a cell phone.[3] Of those individuals, 68% of them own a smartphone.[4] Today, 73% of American adults own a desktop/laptop computer and 45% own a tablet computer.[5] 84% of American adults use the Internet.[6] We truly do live digital lives.[7] Considering these statistics, it is no wonder that the

---

1 Richard J. Schneider, *Thoreau's Life*, The Thoreau Society (last visited November 22, 2016) http://www.thoreausociety.org/life-legacy.

2 Associated Press, *Growing Dependence On Technology Raises Risks of Malfunction*, Crain's New York Business (July 9, 2015) http://www.crainsnewyork.com/article/20150709/TECHNOLOGY/150709895/growing-dependence-on-technology-raises-risks-of-malfunction.

3 Pew Research Center, *Mobile Technology Fact Sheet* (December 27, 2013) http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

4 Monica Anderson, *The Demographics of Device Ownership*, Pew Research Center (October 29, 2015) (This figure constitutes a 33% increase from mid-2011) http://www.pewinternet.org/2015/10/29/the-demographics-of-device-ownership/.

5 Monica Anderson, *Technology Device Ownership: 2015*, Pew Research Center (October 29, 2015) http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

6 Andrew Perrin and Maeve Duggan, *Americans' Internet Access: 2000-2015*, Pew Research Center (June 26, 2015) http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/.

7

collection of digital evidence has become essential to law enforcement.[8] This is particularly true in cases involving child pornography.[9]

However, what about cases in which private individuals discover incriminating evidence on their own? This often occurs in cases involving child pornography and raises challenging Fourth Amendment questions. For instance, when a private party searches a computer, sees a suspicious file, and reports the finding to the police, what kind of government search of the computer may take place? Do police exceed the scope of the warrantless "private search doctrine," which allows them to verify the illegality of evidence discovered by a private party, if they open files other than those originally opened by the third party? Answering these questions become more complicated after the Supreme Court's decision in *Riley v. California*.[10]

This paper will first examine the background Fourth Amendment principles and the development of the private search doctrine. Then this paper will analyze the ways in which the private search doctrine is applied to the digital world. Third, this paper will analyze the Supreme Court's decision in *Riley* and its impact on the application of the private search doctrine in cases involving digital data. Lastly, the author calls for the United States Supreme Court to take action and settle the current circuit split.

Janna Anderson and Lee Rainie, *Digital Life in 2025*, Pew Research Center (March 11, 2014) (noting that experts predict the Internet will become "'like electricity' – less visible, yet more deeply embedded in people's lives for good and ill") http://www.pewinternet.org/2014/03/11/digital-life-in-2025/

8 *See* Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System*, National Criminal Justice Reference Service, at 1 (last visited November 11, 2016) (modern devices serve as huge repositories of personal information yet be carried in a pocket and accessed with a single hand or even voice command) https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf

9 Id. at 7.

10 *Riley v. California*, 134 S. Ct. 2473, 2485 (2014) (police officers may not search an individual's cellphone incident to arrest and must generally secure a warrant before conducting a search of an arrestee's cell phone).

Please note: Many of the cases analyzed herein involve sensitive and often disturbing facts. The author is cognizant of that. Accordingly, the author did his best to balance the need for the requisite factual detail required in any Fourth Amendment analysis with the realities of each case.

I. The Fourth Amendment and The Private Search Doctrine

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizure, shall not be violated…*[11]

The Fourth Amendment of the United States Constitution protects individuals and their property from unreasonable searches and seizures.[12] In *Katz v. United States*, the Supreme Court held that the Fourth Amendment "protects people, not places."[13] In order for a search to implicate the Fourth Amendment, it must violate an individual's legitimate expectation of privacy.[14] In his often-citied concurrence, Justice Harlan articulated a two-pronged test to assess whether an individual has a legitimate expectation of privacy.[15] First, an individual must have

---

11 U.S. Const. amend. IV.

12 Id.

13 Katz v. United States, 389 U.S. 347, 351 (1967).

14 *See* United States v. Jacobsen, 466 U.S. 109, 120 (1971) (holding that a search did not violate the Fourth Amendment because it "infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment).

15 *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring) (explaining that a "twofold requirement" is utilized to determine whether an individual's expectation of privacy is reasonable); *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) (stating that the Harlan test "embraces two discrete questions"); Thomas K. Clancy, *The Search and Seizure of Computers and Electronic Evidence: The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 Miss. L.J. 193, 221 (Fall 205) ("A person seeking to challenge the propriety of a governmental search must establish that she has a protected interest, which the Supreme Court measures by ascertaining whether she ahs a legitimate expectation of privacy that has been invaded by the government.").

exhibited an actual expectation of privacy – the subjective prong – and second, that expectation must be recognized by society as reasonable – the objective prong.[16] Today, the Supreme court states that a Fourth Amendment search does not occur unless "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable."[17]

Under the Fourth Amendment's Warrant Clause, warrantless searches are considered per se unreasonable.[18] However, the Supreme Court has adopted some limited exceptions to the warrant requirement.[19] Generally, a warrantless search will only be upheld if the government's interest in gathering or preserving evidence outweighs an individual's privacy interest.[20] The Fourth Amendment's Exclusionary Rules generally establish that evidence obtained, as the result

---

16 *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be on that society is prepared to recognize as "reasonable."); *see also* Priscilla Grantham Adams, *Fourth Amendment Applicability: Private Searches*, National Center for Justice and Rule of Law, http://www.olemiss.edu/depts/ncjrl/pdf/PrivateSearchDoctrine.pdf (last visited Oct. 17, 2016); Marc Palumbo, *Note: How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 Fordham Urb. L.J. 977, 982 (2009).

17 Kyllo v. United States, 533 U.S. 27, 33 (2001) (quoting California v. Ciraolo, 476 U.S. 207, 211 (1976)).

18 *See* U.S. Const. amend. IV. ("[N]o warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to see seized."); *Katz*, 389 U.S. at 357 ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate are per se unreasonable under the Fourth Amendment -- subject only to a few specially established and well-delineated exceptions.").

19 *See, e.g.*, Washington v. Chrisman, 455 U.S. 1, 5-6 (applying the plain view exception to law enforcement search of dorm room); Chimel v. California, 395 U.S. 752, 762-63 (1969) (adopting the search incident to arrest exception and stating that it is reasonable for law enforcement to search a person being lawfully arrested for weapons or evidence); Carroll v. United States, 267 U.S. 132, 155 (1925) (creating the motor vehicle exception, which allows police to search a motor vehicle based on probable cause that contraband or relevant evidence will be uncovered).

20 *See* Riley v. California, 134 S. Ct. 2473, 2478 (2014) ("the Court generally determines whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is need for the promotion of legitimate governmental interests.'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))).

of an unlawful search, is not admissible against a criminal defendant.[21] However, the pervious considerations are irrelevant unless a government agent conducts the challenged search.[22]

The Fourth Amendment is not implicated unless the government or one of its agents conducts the search in question.[23] Accordingly, an unreasonable search or seizure conducted by a private individual does not violate the Fourth Amendment.[24] Therefore, as long as the private individual conducting the search is not acting as an agent for the government, the discovered evidence is admissible against a criminal defendant.[25] Consequently, the private search doctrine implicates two relevant considerations: (1) whether the searching party is a private individual or government agent, and (2) how far beyond the scope of the initial search can law enforcement go without obtaining a warrant. The following sections address each of these considerations in turn.

A. The Government Agent Test

Determining whether an individual is acting as a government agent or private actor is a case-by-case inquiry, which considers the totality of the circumstances.[26] Reviewing courts will consider (1) whether the government knew of, acquiesced, instigated, compensated or otherwise encouraged the search, and (2) whether the private actor's purpose was to assist law

---

21 *See* Mapp v. Ohio, 367 U.S. 643, 656 (1961)(holding that evidence obtained in searches and seizures that violate the Fourth Amendment is inadmissible).

22 *See* Burdeau v. McDowell, 256 U.S. 465 (1921) (noting that the Fourth Amendment protects against unlawful searches and seizures and that protection applies only to governmental action).

23 Id.

24 *See Jacobsen*, 466 U.S. at 113 (explaining that Fourth Amendment protections do not apply to unreasonable searches by a private individual).

25 *See Coolidge*, 403 U.S. 443, 487-90 (1971).

26 *See* Skinner v. Railway Labor Executives' Ass'n., 489 U.S. 602, 614-15 (1989); *See also* Adams, *Fourth Amendment Applicability: Private Searches*, National Center for Justice and Rule of Law, http://www.olemiss.edu/depts/ncjrl/pdf/PrivateSearchDoctrine.pdf (last visited Oct. 17, 2016).

enforcement.[27] Generally, "mere knowledge and passive acquiesce by the government" is not enough.[28] Kiel Brennan-Marquez, Postdoctoral Research Fellow at NYU's Information Law Institute and Visiting Fellow at Yale Law School's Information Society Project, describes the second criterion of the test to largely be a "mirage[.]"[29] He explains that because the test is derived from common law agency principles, "A does not become B's agent simply because A acts: (1) in a way to benefit B; and (2) out of a desire to benefit B."[30] Instead, there must be some action on B's part.[31] Therefore, Brennan-Marquez concludes that it is hardly surprising that a Fourth Amendment test patterned on agency principles would "inspire courts to treat prodding by law enforcement (of some kind) as a necessary, if not always sufficient, condition of state action."[32]

---

27 United States v. Reed, 15 F.3d 928, 931 (9th Cir. 1994) ("The general principles for determining whether a private individual is acting as a governmental instrument or agent for Fourth Amendment purposes has been synthesized into a two part test. According to this test, we must inquire: (1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends."); *see also*, Kiel Brennan-Marquez, *Article: Outsourced Law Enforcement*, 18 U. Pa. J. Const. L. 797, 806 (2016) (analyzing the development of the private search doctrine and interpretation of the government agent test by the lower courts).

28 *See, eg.*, United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996) (holding that a government agent must be involved directly as a participant, not a mere witness, or indirectly as an encourager of the private person's search); United States v. Crowley, 285 F.3d 553, 558 (7th Cir. 2002) (noting a key factor of the test is whether the government requested the action or offered the individual a reward).

29 Kiel Brennan-Marquez, *Article: Outsourced Law Enforcement*, 18 U. Pa. J. Const. L. 797, 806 (2016).

30 *Id*. (citing United States v. Ellyson, 326 F.3d 522, (4th Cir. 2003) (looking to the "common law of agency" to determine whether a private actor was operating as a state agent)).

31 Id. (citing 19 Williston on Contracts § 54:14 (4th ed. 2015) (explaining that "the relationship of principal and agent…requires mutual consent," and in particular that it "turns on the intentions and actions of the putative principal, not the agent.")).

32 *Id*. at 807.

The Supreme Court first introduced the concept of the private search doctrine in *Coolidge v. New Hampshire*.[33] In this case, police suspected that Edward Coolidge was involved with the kidnapping and murder of a fourteen-year-old girl, Pamela Mason.[34] After learning that Coolidge had been away from home on the evening of Mason's disappearance, the police went to the Coolidge residence to question him.[35] During the initial interview, Coolidge denied any wrongdoing and voluntarily surrendered two shotguns and a rifle to the police.[36] He also agreed to take a lie-detector test concerning his statements regarding his whereabouts on the night of Mason's disappearance.[37]

On the following Sunday, Coolidge reported to the police station where the lie detector would be administered, while two plainclothes policemen went to the Coolidge residence.[38] There, the plainclothes officers encountered Mrs. Coolidge and informed her that her husband was in "serious trouble."[39] The officers proceeded to question Mrs. Coolidge, who voluntarily turned over four guns and some clothes she believed her husband was wearing on the evening of

---

33 Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) ("Had Mrs. Coolidge, wholly on her own initiative, sought out her husband's guns and clothing and then taken them to the police station to be used as evidence against him, there can be no doubt under existing law that the articles would later have been admissible in evidence.").

34 *Id*. at 445.

35 Id.

36 Id.

37 Id.

38 *Id*. at 446.

39 Id.

Mason's disappearance.[40] The evidence incriminated Coolidge, who was ultimately convicted of kidnapping and murder and sentenced to life in prison.[41]

Prior to his conviction, Coolidge moved to suppress the evidence voluntarily surrendered to law enforcement by his wife.[42] Coolidge argued that his wife was acting as an "instrument" of law enforcement when she brought out his guns and clothing and handed them over to the officers.[43] Therefore, Coolidge asserted that he was the victim of an unlawful search and seizure.[44] The Supreme Court rejected Coolidge's argument and upheld the denial of his motion to suppress.[45]

The *Coolidge* Court found that the officers did not "coerce or dominate" Mrs. Coolidge in any way.[46] Instead, they stated that the officers did nothing more than direct her actions by the "more subtle techniques of suggestion that are available to officials in circumstances like these."[47] The Court noted that to hold otherwise would be "to hold, in effect, that a criminal suspect has constitutional protection against the adverse consequences of a spontaneous, good-faith effort by his wife to clear him of suspicion."[48] The Court explained further that it is not part of the underlying policy of the Fourth Amendment to "discourage citizens from aiding to the

---

40 Id.

41 *Id*. at 448.

42 *Id*. at 487.

43 Id.

44 Id.

45 *Id*. at 489.

46 Id.

47 *Id*. at 489-90.

48 *Id*. at 490.

utmost of their ability in the apprehension of criminals."[49] The *Coolidge* Court made clear that the Fourth Amendment was not triggered in this case.[50]

The Supreme Court limited the private search doctrine in its decision in *Skinner v. Railway Labor Executives' Labor Association*.[51] In *Skinner*, the Court considered regulations promulgated after the passage of the Federal Railroad Safety Act of 1970 to combat problems of alcohol and drug abuse by railroad employees.[52] The regulations made post-accident toxicological testing mandatory.[53] Accordingly, the railroad companies were obligated by the regulations to collect blood and urine samples after the occurrence of any number of railway incidents.[54] Numerous employees and labor unions challenged the regulations as a violation of their Fourth Amendment rights.[55]

The *Skinner* Court first considered whether the Fourth Amendment was implicated by these tests.[56] The Court held that the breath and urine tests required by the railroad companies in compliance with the regulations are searches that implicate the Fourth Amendment.[57] The Court

---

49 Id.

50 Id.; *see also* Kiel Brennan-Marquez, *Article: Outsourced Law Enforcement*, 18 U. Pa. J. Const. L. 797, 802 (2016) ("In short, when Mrs. Coolidge provided evidence to the police, she was acting of her own volition, not as an instrument of the state. So the Fourth Amendment, far from being violated, was not even triggered.).

51 Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989).

52 *Id*. at 606-07.

53 *Id*. at 609.

54 Id.

55 *Id*. at 612.

56 *See Id*. at 613-14 ("Before we consider whether the tests in question are reasonable under the Fourth Amendment, we must inquire whether the tests are attributable to the Government or its agents, and whether they amount to searches or seizures.").

57

further stated that private actors become agents or instruments of the state if they are legally required to perform such searches.[58] Justice Kennedy, writing for the Court, explained to hold otherwise would allow legislative bodies to circumvent Fourth Amendment protection at will by deputizing private actors to perform searches that would otherwise fall to law enforcement.[59] Government action that is not compelled may still qualify as a Fourth Amendment search, if the government "removes all legal barriers to [a given type of search] and indeed [makes] plain not only its strong preference for [searches], but also its desire to share the fruits of [the] intrusions."[60] While the *Skinner* Court ultimately upheld the regulations as constitutional,[61] the decision limited the private search doctrine in explaining that a seemingly private actor may become a de facto government agent by complying with government regulations.[62]

B. How Far Is Too Far?: Defining The Scope Of Law Enforcement's Subsequent Warrantless Search

---

Id. at 614.

58 *Id*. at 614-16 ("The fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one. Here, specific features of the regulations combine to convince us that the Government did more than adopt a passive position toward the underlying private conduct.").

59 *Id*. at 615-16 ("In light of these provisions, we are unwilling to accept petitioners' submission that tests conducted by private railroads in reliance on Subpart D will be primarily the result of private initiative."); *see also* Kiel Brennan-Marquez, *Article: Outsourced Law Enforcement*, 18 U. Pa. J. Const. L. 797, 803 (2016)

60 *Skinner*, 489 U.S. at 615.

61 *Id*. at 633. ("We conclude that the compelling Government interests served by the FRA's regulations would be significantly hindered if railroads were required to point to specific facts giving rise to a reasonable suspicion of impairment before testing a given employee. In view of our conclusion that, on the present record, the toxicological testing contemplated by the regulations is not an undue infringement on the justifiable expectations of privacy of covered employees, the Government's compelling interests outweigh privacy concerns.").

62 *Id*. at 615-16. ("The Government has removed all legal barriers to the testing authorized by Subpart D, and indeed has made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions. In addition, it has mandated that the railroads not bargain away the authority to perform tests granted by Subpart D. These are clear indices of the Government's encouragement, endorsement, and participation, and suffice to implicate the Fourth Amendment.").

In *Walter v. United States*, the Supreme Court considered a "bizarre" set of facts that implicated the Fourth Amendment's private search doctrine.[63] In this case, a shipment containing 871 boxes of eight-millimeter film was sent from St. Petersburg, Florida, to Atlanta, Georgia.[64] The package was addressed to "Leggs, Inc.[,]" but was mistakenly delivered to "L'Eggs Products, Inc."[65] Upon arrival, L'Eggs Products' employees inspected the shipment and its contents.[66] The boxes' labels displayed "suggestive drawings" of homosexual sexual activity and "explicit descriptions" of their contents.[67] One of the employees then opened one or two of the boxes and unsuccessfully attempted to view portions of the film by holding it up to the light.[68] The employees then contacted the Federal Bureau of Investigations ("FBI"), who subsequently seized the films.[69] The FBI then viewed the films with a projector "without making any effort to obtain a warrant or to communicate with the consignor or the consignee of the shipment."[70] Petitioners were subsequently indicted and convicted on obscenity charges relating to the interstate transportation of the films after their motion to suppress evidence of the films was denied.[71]

---

63 Walter v. United States, 447 U.S. 649, 651 (1980).

64 *Id*. at 651.

65 Id.

66 Id.

67 *Id.* at 652.

68 Id.

69 Id.

70 Id.

71 Id.

The Supreme Court granted certiorari and reversed the convictions after finding that the FBI's "unauthorized exhibition of films constituted an unreasonable invasion of their owner's constitutionally protected interest in privacy."[72] Justice Stevens, writing on behalf of the majority, noted that it was "perfectly obvious" that the agents' reason for viewing the films was to determine whether the owner was guilty of a federal crime.[73] However, while the labels gave the agents probable cause to believe the films were obscene they were not sufficient to support a conviction.[74] Justice Stevens took care to note that just because the FBI agents lawfully possessed the films, they did not automatically have authority to search their contents."[75] Additionally, the fact that the packages had been opened by a private party before they were acquired by the FBI does not "excuse the failure to obtain a search warrant."[76] While the private search by the L'Eggs employees "frustrated that expectation in part[,]" it did not "simply strip the remaining unfrustrated portion of that expectation of all Fourth Amendment protection."[77]

Nearly forty years later, in *United States v. Jacobsen*, the Supreme Court held that a government agent's warrantless search does not violate the Fourth Amendment if it is simply a replication of a search already conducted by a private party.[78] In *Jacobsen*, Federal Express

---

72 *Id*. at 654.

73 Id.

74 Id.

75 Id. ("Ever since 1878 when Mr. Justice Field's opinion for the court in *Ex parte Jackson*, 96 U.S. 727, established that sealed packages in the mail cannot be opened without a warrant, it has been settled than an officer's authority to possess a package is distinct from his authority to examine its contents.").

76 *Id*. at 656.

77 Id.

78 *See* United States v. Jacobsen, 466 U.S. 109, 116-19 (1984) (describing the standard for analyzing warrantless searches by a government agent of an item already searched by a party); *See also* Katie Matejka, *Note:*

("FedEx") employees working at Minneapolis-St. Paul Airport accidently damaged and tore a package with a forklift.[79] Pursuant to company policy, an office manager inspected the damaged package and opened it to examine the contents.[80] Inside, the office manager discovered four zip-lock plastic bags containing about six and a half ounces of white powder.[81] Suspecting the substance to be cocaine, the FedEx employees notified the Drug Enforcement Administration (DEA).[82]

The first DEA agent arrived, inspected the package and performed a field test of the white powdery substance, confirming it to be cocaine.[83] A short time later, more DEA agents arrived, inspected the package for themselves and performed another field test, which confirmed the results of the initial field test.[84] The DEA agents then obtained a warrant to search the place where the package was addressed, executed the warrant, and arrested Jacobsen.[85] The United States District Court of Minnesota declined to suppress the evidence and Jacobsen was convicted of possession with intent to distribute.[86] Jacobsen appealed to the United States Court of Appeals

---

United States v. Lichtenberger: The Sixth Circuit Improperly Narrowed The Private Search Doctrine Of The Fourth Amendment In a Case of Child Pornography On A Digital Device, 49 Creighton L. Rev. 177, 180 (2015); This paper does not comment of the Supreme Court's introduction and perceived expansion of the private search doctrine. For an interesting criticism of the Court's decision in *Jacobsen* please see Kim A. Lambert, *United States v. Jacobsen: Expanded Private Search Doctrine Undermining Fourth Amendment Values*, 16 Loy. U. Chi. L.J. 359 (1985).

79 *Jacobsen*, 466 U.S. 109, 111 (1984).

80 Id.

81 Id.

82 Id.

83 Id.

84 *Id*. 111-12.

85 Id.

86 *Jacobsen*, 683 F.2d 296, 298 (8th Cir. 1982).

for the Eighth Circuit.[87] The Eighth Circuit focused primarily on the agents' field tests.[88] The court ultimately reversed Jacobsen's conviction, ruling that the field test expanded the private search and required a warrant.[89] The Supreme Court granted certiorari.[90]

In reversing the Eighth Circuit, the Supreme Court focused entirely on the initial search conducted by the FedEx employees.[91] The Court reasoned that the DEA agents' subsequent field tests did not require a warrant because the "initial invasion" of Jacobsen's package occurred during a private search.[92] Therefore, according to Justice Stevens, even though the field tests exceed the scope of the private search, it was not a search under *Katz*, because it could "not compromise any legitimate expectation of privacy."[93] The positive test did not remove the reasonable expectation of privacy; instead that fact that whatever the white powder turned out to be was no longer a "private fact" there was no longer a reasonable expectation of privacy in it.[94] The Court was not willing to accept Jacobsen's argument that the office manager's decision to contact federal authorities made him a government actor.[95] Further, the Court declared that the

---

87 *Id*. at 299-300.

88 Id.

89 Id.

90 *Jacobsen*, 466 U.S. at 112-13.

91 *Id*. at 115.

92 Id.

93 Id.

94 *Id.* at 123.

95 *See Id*. at 114-15 ("The fact that agents of the private carrier independently opened the package and made an examination that might have been impermissible for a government agent cannot render otherwise reasonable official conduct unreasonable…[Here] the initial invasions of respondents' package were occasioned by private action.").

motivation behind the employees' conduct was irrelevant in applying the private search doctrine.[96]

II. Applying The Private Search Doctrine To The Digital World

The private search doctrine has justified searches in the digital world in a number of different contexts.[97] The most common cases include computer repairpersons,[98] hacktivists,[99] and Internet service providers[100]. The following cases illustrate different ways in which state and federal courts of appeals have applied the private search doctrine in these instances.

A. The Computer Repairperson

In *State v. Lasaga*, the Supreme Court of Connecticut upheld the conviction of a college professor whose computer download history was monitored and reported by a student employed by the university to law enforcement.[101] Professor Lasaga was employed by Yale University as a

---

96 *See Id*. at 115 (it is irrelevant whether the intrusion was "accidental or deliberate").

97 *See e.g.*, State v. Horton, 962 So.2d 459, 463 (La. App. 2 Cir. 2007) (computer repairman discovering evidence of child pornography in the ordinary course of business is not a search under the Fourth Amendment); State v. Lasaga, 848 A.2d 1149 (Conn. 2004) (student employed by a university as a computer technician was not acting as a government agent when he monitored defendant's computer and reported that he was downloading child pornography); United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003) (computer hacker acted as a private citizen when they hacked into defendant's computer and provided law enforcement with evidence of child pornography); United States v. Stevenson, 727 F.3d 826, 829-30 (8th Cir. 2013) (holding that AOL was operating as private actor, not a state agent, when it decided to has email traffic for child pornography and other contraband); United States v. Richardson, 607 F.3d 357, 366-67 (4th Cir. 2010) (holding same).

98 *See Lasaga*, 848 A.2d 1149 (Conn. 2004); *Horton*, 962 So.2d 459, 463 (La. App. 2 Cir. 2007).

99 *See Jarrett*, 338 F.3d 339, 344 (4th Cir. 2003).

100 *See Stevenson*, 727 F.3d 826, 829-30 (8th Cir. 2013).

101 *Lasaga*, 848 A.2d 1149 (Conn. 2004).

professor of geology and geophysics.[102] On October 23, 1998, Victor Sletten, a Yale graduate student, informed Pal Gluhosky, a Yale employee responsible for ensuring that the geology department computers were functioning properly, that another student told him that Professor Lasaga downloaded child pornography onto his geology department office computer.[103] Gluhosky decided to monitor Professor Lasaga's download history.[104] From October 23 through October 30, 1998, Gluhosky monitored Professor Lasaga's download activity and suspected that the Professor was in fact downloading child pornography.[105] Gluhosky communicated his suspicions to his supervisors and was instructed to continue his activities.[106]

On November 3, Gluhosky provided law enforcement with hard copies of computer logs detailing Lasaga's computer activities and a CD that contained copies of images that the defendant had downloaded to a computer in the geology department.[107] This information was subsequently turned over to the FBI.[108] Based on Gluhosky's information, federal officials obtained a search warrant for Professor Lasaga's residence.[109] During the search, FBI agents seized Lasaga's computer, zip drives, floppy discs, compact discs, two homemade videotapes, and other items.[110] Based on this evidence, Lasaga was charged with two counts of sexual assault

---

102 *Id*. at 1152.

103 Id.

104 Id.

105 Id.

106 Id.

107 Id.

108 *Id*. at 1153.

109 *Id*. at 1153-54.

110

in the first degree, two counts of promoting a minor in an obscene performance, and two counts of risk of injury to a child.[111] Lasaga filed a motion to suppress the evidence seized during the FBI's search, which was denied by trial court denied.[112] Lasaga then pled, but reserved the right to appeal the denial of his motion to suppress.[113]

In upholding the trial court's denial of Lasaga's motion to suppress, the Supreme Court of Connecticut agreed that Gluhosky's actions did not implicate the Fourth Amendment as he was acting as a private party while monitoring Lasaga's computer activities.[114] The court found that the record supports the trial court's conclusion that "Gluhosky was in no way acting as an agent of the government in obtaining the information and material which was utilized by [the FBI] in drafting the search warrant."[115] The police did not seek out Gluhosky and were not involved in his decision to obtain information regarding Lasaga's computer activities.[116] The court also emphasized that Gluhosky had no previous connection with the police and received nothing in return for his cooperation.[117] While there was a dispute in the record regarding whether law enforcement asked Gluhosky to continue to monitor Lasaga and provide them with information or whether Gluhosky independently decided to do so, the court was indifferent as to the

---

Id. at 1154.

111 Id.

112 Id.

113 *Id*. at 1154-55.

114 *Id*. at 1157

115 Id.

116 Id.

117 Id.

significance of this discrepancy.[118] The court ultimately determined that "police involvement was not so extensive as to have created an agency relationship between Gluhosky and the police."[119]

Similarly, in *State v. Horton*, The Second Circuit Court of Appeal for Louisiana found that a computer repairman's actions in the ordinary course of business did not qualify as a search under the Fourth Amendment.[120] In this case, Robert Horton took his computer to a local Best Buy for repairs.[121] Horton instructed the computer technician, Christopher Stoll, to install a new hard drive, but not to remove the old one.[122] After installing the new hard drive, Stoll followed Best Buy's "post-op procedure" to see if he could repair issues related to problems with the computer's power button and monitor display "flickering and shaking."[123] In doing so, Stoll decided to view an image from his own thumb drive, as was common procedure used by Best Buy technicians.[124] Stoll then accessed the Microsoft Paint program to open the media file.[125] When Stoll opened Microsoft paint a default picture directory entitled "My Pictures" automatically opened and Stoll saw six thumbnail pictures of nude children engaged in sexual

---

118 Id.

119 Id.

120 State v. Horton, 962 So. 2d 459, 466 (La. App. 2 Cir. 2007) (concluding that law enforcement agent's viewing of additional images did not taint the original warrantless viewing of the images upon which the search warrant was issued).

121 *Id*. at 461.

122 Id.

123 Id.

124 Id.

125 Id.

acts.[126] Stoll immediately alerted other Best Buy employees and they decided to call the police.[127]

District Attorney investigator and computer forensics expert, Mark Fargerson, responded to the call and the Best Buy employees showed him the images they discovered.[128] Fargerson then viewed additional images and determined they were in fact child pornography.[129] This information was then used to obtain a search warrant for Horton's computer.[130] The subsequent search revealed over 100 pages of child pornography.[131] Horton filed a motion to suppress the evidence, arguing that the "court should set some guidelines in what is a permissible private search by a computer technician."[132] Horton also argued that Fargerson exceeded the scope of the private search by the Best Buy employees because he "did additional procedures in opening and enlarging the photos[.]"[133]

The trial court denied Horton's motion to suppress and Horton appealed.[134] The appellate court agreed with the trial court's denial of Horton's motion to suppress.[135] The court noted that there is "no merit" to Horton's argument that the Best Buy employees were acting on behalf of

---

126 Id.

127 Id.

128 Id.

129 Id.

130 Id.

131 *Id*. at 462.

132 Id.

133 Id.

134 *Id*. at 463.

135 Id.

law enforcement.[136] The court found that the discovery of the unlawful pornographic images by the Best Buy employees was "inadvertent and unexpected."[137] Accordingly, the search qualified as a private search because it not connected to state authority in any way.[138]

B. The Hacktivist

Hacktivism is the act of hacking a website or computer network in an effort to convey a social or political message.[139] Unlike malicious hackers, who invade computers or networks with the intent to cause harm, the hacktivist is usually motivated by a desire to serve a social cause.[140] A well-known example is the hacker group, Anonymous.[141] In 2015, the group announced "Operation Death Eaters" in the wake of the Westminster child abuse scandal[142] in London.[143] In doing so, Anonymous vowed to target anyone connected to the scandal as well as the general child porn issue that was overwhelming British authorities.[144] Similarly, in *United States v.*

---

136 *Id*. at 464.

137 Id.

138 Id.

139 Technopedia, *Hactivism* (last visited November 17, 2016), www.technopedia.com/definition/2410/hacktivism.

140 Id.

141 Peter Foster, *Anonymous Hacks Turn Fire On Global Pedophile Menace*, The Telegraph (January 23 2015) http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11363303/Anonymous-hackers-turn-fire-on-global-paedophile-menace.html.

142 Steven Swinford, *Secret Government Filed On 'Unnatural' Sexual Behaviour At Westminster Unearthed*, The Telegraph (January 21, 2015) http://www.telegraph.co.uk/news/uknews/crime/11359459/Secret-government-file-on-unnatural-sexual-behaviour-at-Westminster-unearthed.html

143 Foster, *Anonymous Hacks Turn Fire On Global Pedophile Menace*, The Telegraph (January 23 2015)

144 Id.

Jarrett, the FBI and local enforcement agents received incriminating information via email from a hacker known only as "Unknownuser".[145]

Beginning in July 2000, Unknownuser began to supply federal and state officials with information related the downloading and sharing of child pornography.[146] Dr. Bradley Steiger was the first individual Unknownuser exposed to the FBI.[147] Unknownuser gained entry into Steiger's computer via a "Trojan Horse"[148] program attached to a picture Unknownuser posted to a news group frequented by pornography enthusiasts.[149] Once Steiger downloaded the picture to his own computer, the Trojan horse program was also downloaded and Unknownuser was able to enter Steiger's computer undetected.[150] Unknownuser then searched Steiger's hard drive and found evidence of child pornography, which he supplied to law enforcement.[151]

---

145 United States v. Jarrett, 338 F.3d 339, 341 (4th Cir. 2003) (Unknownuser identified himself only as someone "from Istanbul, Turkey," who could not "afford an overseas phone call and cannot speak English fluently").

146 Id.

147 *See* United States v. Steiger, 318 F.3d 1044 (11th Cir. 2003).

148 A Trojan horse ("Trojan") is one of the most popular methods used by hackers and cybercriminals alike to gain access into an unsuspecting computer. The term comes from the well-known Greek fable, in which the Greeks presented the Trojans with a giant wooden horse as a peace offering. Unbeknownst to the Trojans, the hollow wooden horse concealed Greek soldiers who eventually sprung out and assisted the Greeks in sacking Troy. Similarly, a Trojan Horse program presents itself as a helpful computer program while hiding its true purpose. They can be delivered to users through email or can be attached to files made available on the Internet for download. After it is installed, the Trojan can remain in the system undetected; allowing a third party to access files, copy or even delete data without being detected. *See* Crimeware: Trojans & Spyware, Norton (last visited November 20, 2016), https://us.norton.com/cybercrime-trojansspyware.

149 *Jarrett*, 338 F.3d at 341.

150 Id.

151 Id.

In November 2000, FBI Special Agent Duffy attempted to convince Unknownuser to reveal his identity and testify in Steiger's case.[152] Despite Agent Duffy's assurances that Unknownuser would not be prosecuted for his hacking activities, Unknownuser refused to testify.[153] After repeated failed attempts to convince Unknownuser to testify, Agent Duffy thanked Unknownuser for his assistance and stated, "[i]f you want to bring other information forward, I am available."[154]

Unknownuser did not contact law enforcement officials again until December 2001, when he sent an unsolicited email to law enforcement in Alabama.[155] Unknownuser informed law enforcement that he had "found another child molester[,]" who he identified as William Jarrett.[156] On December 4, 2001, Unknownuser sent thirteen email messages to law enforcement; including a "ten-part series of email with some forty-five attached files containing the 'evidence' that Unknownuser had collected on Jarrett."[157] Jarrett was indicted and arrested shortly thereafter.[158] As before, FBI Agent Duffy again contacted Unknownuser and thanked him for his assistance in identifying Jarrett.[159] Unknownuser and Agent Duffy exchanged emails and Agent

---

152 Id.

153 Id.

154 Id.

155 *Id*. at 342.

156 Id.

157 Id.

158 Id.

159 Id.

Duffy encouraged Unknownuser to remain in contact with a fellow agent, Agent Faulkner, via her personal email address.[160]

After being indicted on child pornography charges, Jarrett moved to suppress the evidence obtained against him.[161]The district court denied the motion and Jarrett entered a conditional guilty plea.[162] Prior to sentencing however, Jarrett reconsidered his earlier motion to suppress on the basis of new evidence revealing a series of emails exchanged between Unknownuser and FBI Agent Faulkner, begging shorty after Jarrett's arrest.[163] The government did not disclose these emails until after Jarrett entered his guilty plea.[164] Specifically, Jarrett pointed to a series of emails dated December 19, 2001, in which Agent Faulkner explicitly thanked Unknownuser for providing the information to law enforcement.[165]

Over the next few months, Agent Faulkner and Unknownuser maintained what the district court described as a "pen-pal" type correspondence.[166] Agent Faulkner repeatedly expressed thanks and even admiration for Unknownuser's assistance.[167] Unknownuser told Agent Faulkner that he would continue his hacking activities and Agent Faulkner never discouraged that.[168] Upon consideration of the series of emails, the district court reversed its

---

160 Id.

161 Id.

162 Id.

163 Id.

164 *Id*. at 342-43.

165 *Id*. at 343 (the court described the exchange as the proverbial "wink and a nod").

166 Id.

167 Id.

168

earlier decision and suppressed the evidence.[169] In doing so, the court reasoned that the "totality of all the contact between law enforcement and Unknownuser encouraged Unknownuser to continue his behavior and to remain in contact with the FBI."[170] The district court concluded that the Government and Unknownuser had "expressed their consent to an agency relationship[]" and the evidence obtained on the basis of Unknownuser's hacking activities violated Jarrett's Fourth Amendment rights.[171] The government appealed.[172]

The 4th Circuit Court of Appeals relied on the Supreme Court's decisions in *Coolidge* and *Skinner* in describing the private search doctrine and setting out the government agent test.[173] While the Government conceded that Unkownuser intended to assist law enforcement, it argued that the Government did not know or acquiesce in Unknownuser's search "in a manner sufficient to transform Unknownuser into an agent of the Government" to make the search unconstitutional.[174] The burden is placed on the defendant to "demonstrate that the Government knew of and acquiesced in the private search and that the private individual intended to assist law enforcement authorities.[175] However, the 4th Circuit noted that they have "required evidence of

---

Id.

169 Id.

170 Id.

171 Id.

172 *Id*. at 344.

173 Id. "Tbe Fourth Amendment protects against unreasonable searches and seizers by Government officials and those private individuals actins as "instruments or agents" of the Government." (quoting *Coolidge*, 403 U.S. 443, 487 (1971)); "Determining whether the requisite agency relationship exists 'necessarily turn on the degree of the Government's participation in the private party's activities,…a question that can only be resolved 'in light of all the circumstances." (quoting *Skinner*, 489 U.S. 602, 614-15 (1989)).

174 *Id*. at 344-45.

175 *Id*. at 345.

more than mere knowledge and passive acquiesce by the Government before finding an agency relationship."[176] With these principles in mind, the 4th Circuit rejected Jarrett's contentions that Unknownuser was acting as a government agent.[177]

In reversing the district court's decision to suppress the evidence against Jarrett, the 4th Circuit emphasized the fact that Unknownuser's email exchange with Faulkner took place after Unknownuser had hacked into Jarrett's computer and after the "fruits of Unknownuser's hacking" had been made available to the FBI.[178] The court found that Faulkner's "knowledge and acquiescence was entirely post-search."[179] The court reasoned "such after-the-fact conduct cannot serve to transform the prior relationship between Unknownuser and the Government into an agency relationship with respect to the search of Jarrett's computer."[180] While the Government "operated close to the line" in this case, Jarrett failed to "demonstrate the requisite level of knowledge and acquiesce sufficient to make Unknownuser a Government Agent when he hacked into Jarrett's computer."[181] Even though the Government did not "actively discourage" Unknownuser from engaging in illegal hacking this did not transform him into a Government agent.[182] Even though the 4th Circuit described the Government's behavior as "discomforting[,]"

---

176 Id.

177 Id.

178 *Id*. at 346.

179 Id.

180 Id.

181 *Id.* at 347.

182 Id.

they noted that the Government is under no "special obligation" to discourage these types of activities.[183]

C. The Internet Service Provider

AOL is a well-known Internet service provider ("ISP") that provides email and web services to its users.[184] AOL identifies certain files that "may damage its network" with "hash values."[185] A hash value is "an algorithmic calculation that yields an alphanumeric value for a file."[186] Files containing child pornography were amongst those files AOL assigned hash values.[187] During the regular course of business, AOL scans files sent through its network with a tool it calls the "Image Detection and Filtering Process."[188] When the program detects files with a hash value associated with child pornography, it automatically forwards a report to the National Center for Missing and Exploited Children.[189]

In September 2010, the filtering program triggered an alert for images depicting child pornography being sent from the e-mail account of Jeremy Stevenson.[190] Law enforcement officials obtained a search warrant for Stevenson's home and eventually uncovered a large

---

183 Id. ("[a]lthough evidence of such 'encouragement' would not have to target a particular individual, it would have to signal affirmatively that the Government would be ready and willing to participant in an illegal search.").

184 United States v. Stevenson, 727 F.3d 826, 828 (8th Cir. 2013).

185 Id.

186 Id.

187 Id.

188 Id.

189 Id.

190 Id.

quantity of child pornography stored on his computers and digital storage devices.[191] Stevenson was indicted on charges of possessing child pornography.[192] Stevenson filed a motion to suppress the images discovered by AOL, arguing that the ISP's scanning of his emails violated his Fourth Amendment rights.[193] The district court denied the motion, explaining that AOL was a private actor and was therefore not constrained by the Fourth Amendment.[194] Stevenson entered a conditional guilty plea, while reserving his right to appeal the district court's denial of his motion to suppress.[195]

On appeal, Stevenson argued that AOL acted as a government agent when it scanned his emails because Title 18, United States Code Section 2258A(a) "requires AOL to report to the National Center [for Missing and Exploited Children] any apparent violation of the child pornography laws that AOL discovers while providing electronic communication services."[196] Relying on the Supreme Court's decision in *Skinner*, Stevenson likened Section 2258A(a) to the testing requirements that made optional tests amount to state action.[197] Additionally, Section 2258B(a) ISPs from suit arising from the performance of the reporting responsibilities implied therein.

---

191 Id.

192 Id.

193 Id.

194 *Id*. at 828-29.

195 *Id*. at 829.

196 Id.

197 Id.

The 8th Circuit summarily rejected this argument and found that the regulations at issue neither authorized AOL to scan its users' emails and did not remove legal barriers to scanning by preempting private contracts that forbid scans.[198] The court concluded that the "only similarity between the statutes that Stevenson cites and the *Skinner* regulations in that both include reporting obligations."[199] However, a reporting requirement, standing alone, "does not transform an Internet service provide into a government agent whenever it chooses to scan files sent on its network for child pornography."[200]

III. *Riley v. California* and the Supreme Court's Push To Protect Data Privacy

In *Riley v. California*, a unanimous Supreme Court held that police officers may not search an individual's cellphone incident to arrest and must generally secure a warrant before conducting a search of an arrestee's cell phone.[201] In *Riley*, the Court considered two cases presenting a common question: do law enforcement agents need to acquire a search warrant before they search an arrestee's cellular phone.[202]

In the first case, David Riley was stopped by a police officer for driving with expired registration tags.[203] During the stop, the officer discovered that Riley's driver's license had been

---

198 *Id*. at 829-30.

199 *Id*. at 830.

200 Id. *See also United States v. Richardson*, 607 F.3d 357, 366-67 (4th Cir. 2010) (holding same).

201 *Riley v. California*, 134 S. Ct. 2473, 2485 (2014).

202 *Id*. at 2480.

203 Id.

suspended.[204] Pursuant to department policy, the officer impounded Riley's vehicle and conducted an inventory search of the car.[205] The officer discovered two handguns hidden under the cars hood and Riley was arrested for unlicensed possession of concealed and loaded firearms.[206] An officer then searched Riley incident to arrest and found evidence associated with the "Bloods" street gang.[207] Upon accessing Riley's smartphone, the officer noticed some words or contacts preceded by the letters "CK" or "Crip Killers."[208] Two hours later, at the police station a detective from the gang squad went through Riley's phone, searching for further evidence of gang affiliation.[209] During the search, the detective found photographs of Riley standing in front of a car they suspected to have been involved in a shooting a few weeks earlier.[210] Riley was subsequently charged in connection with the shooting and sentenced to a term of fifteen years to life in prison.[211]

In the second case, a police officer observed Brima Wurie make a drug sale from his car.[212] After arresting him and brining him to the police station, the officers seized two of Wurie's cellphones.[213] Unlike Riley's case however, Wurie's phone was a "flip phone."[214] The police

---

204 Id.

205 Id.

206 Id.

207 Id.

208 Id.

209 *Id*. at 2480-81.

210 *Id*. at 2481.

211 Id.

212 Id.

213

noticed that Wurie's phone was repeatedly receiving calls from a source identified as "my house" on the phone's external screen.[215] Eventually, the officers opened the phone and observed a photo of a woman and baby set as the phone's wallpaper.[216]After accessing the call log, the police were able determine the phone number associated with the "my house" label and traced it to Wurie's apartment building.[217] The officers went to the building, saw Wurie's name on a mailbox and observed a woman through the window who resembled the wallpaper photo on Wurie's phone.[218] Based on the information from the cellphone and their observations, the officers obtained a search warrant and searched Wurie's apartment.[219] The subsequent search uncovered 215 grams of crack cocaine, marijuana, drug paraphernalia, a firearm and ammunition, and cash.[220] Wurie was convicted of numerous offenses was sentenced to 262 months in prison.[221]

The Supreme Court granted certiorari and consolidated both cases.[222] In describing the social significance of cellphones, the Court characterized them as being a "pervasive and insistent part of daily life."[223] So much so that Chief Justice Roberts quipped that the "proverbial

---

Id.

214 Id. (Court explaining that a flip phone is "a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone.").

215 Id.

216 Id.

217 Id.

218 Id.

219 Id.

220 Id.

221 *Id.* at 2481-82.

222 *Id*. at 2480.

223

visitor from Mars might conclude they were an important feature of human anatomy." [224] While Riley and Wurie utilized phones with "varying levels of sophistication," the *Riley* Court noted that both devices are based on technologies that were "inconceivable" when seminal cases like *Chimel* and *Robinson* were decided.[225] Accordingly, the Court refused to extend the rational of these cases to cell phone searches, instead mandating that officers generally secure a warrant before conducting a search.[226]

The Court observed that cell phones differ in both a quantitative and qualitative sense from other objects that might be carried on an arrestee's person.[227] Considering that the Court described cell phones as "minicomputers" capable of storing immense amounts of data, this conclusion is not surprising.[228] Additionally, the Court noted that cell phones collect many distinct types of data and create numerous privacy issues.[229] With this in mind, the Court declined to extend the primary *Chimel* rationales[230] to this case.[231]

Id. at 2484.

224 Id.

225 Id.

226 *Id*. at 2485; *See also* George M. Dery III and Kevin Meehan, *A New Digital Divide? Considering The Implications Of Riley V. California's Warrant Mandate For Cell Phone Searches*, University of Pennsylvania Journal of Law and Social Change, Vol. 18, Iss. 4, Art. 2 at 322 (2015) (observing that Court's primary focus was on the implication of smart phone technology).

227 *Id*. at 2478.

228 *Id*. at 2489.

229 *Id*. at 2489-91. (noting the cell phones may reveal "detailed information about all aspects of a persons life" through browsing history, geolocation data, and apps.); *see also* Marc Rotenberg and Alan Butler, *Symposium: In Riley V. California, A Unanimous Supreme Court Sets Out Fourth Amendment For Digital Age*, SCOTUSblog, www.scotusblog.com/2014/06symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amednment-for-digitla-age/ (June 26, 2014) (noting that revealing information regarding medical conditions or a certain diseases coupled with visits to WebMD may reveal an individual's private information); Tyler G. Newby, *Litigation Alert: Supreme Court Defends Expectation of Privacy In Cell Phone Data*, Fenwick & West LLP (June 26, 2014) (noting that while dicta the language suggests that individuals have constitutionally protected privacy

First, the Court noted that unlike physical objects, digital data does not pose a risk to officer safety.[232] Second, the Court dismissed the Government's concerns related to evidence preservation.[233] Further, Chief Justice Roberts explained that while *Robinson's* categorical rule allowing searches upon every lawful custodial arrest struck the "appropriate balance in the context of physical objects," its rationales lost logical force with respect to the "digital content on cell phones."[234] Ultimately, the *Riley* Court limited *Robinson's* search incident to arrest rationale in cases involving cell phones.[235] Katie Matejka astutely notes that the *Riley* Court made its holding clear: "it is not the case that cell phones may never be searched by law enforcement – it is that law enforcement must first obtain a warrant to search the cell phone."[236]

IV. The Current Circuit Split: *Riley's* Impact On The Private Search Doctrine

---

interest in each of these categories of information, at least for purposes of a government search of their personal devices)

230 *Chimel*, 395 U.S. 752, 762-63 (1969) (adopting the search incident to arrest exception and stating that it is reasonable for law enforcement to search a person being lawfully arrested for weapons or evidence).

231 *Id*. at 2485.

232 Id. (noting that there was no reason to believe that cell phones regularly alerted officer to the impending arrival of the arrestee's confederates).

233 *Id*. at 2486 (observing that concerns related to remote data wiping and data encryption are not prevalent problems).

234 Id. at 2484-87; *See also* George M. Dery III and Kevin Meehan, *A New Digital Divide? Considering The Implications Of Riley V. California's Warrant Mandate For Cell Phone Searches*, University of Pennsylvania Journal of Law and Social Change, Vol. 18, Iss. 4, Art. 2 at 323(2015) (noting that the *Riley* Court determined that a cell phone search places "vast quantities of person information literally in the hand of individuals" bore "little resemblance to the type of brief physical search considered in *Robinson*).

235 Id.

236 Katie Matejka, *Note: United States v. Lichtenberger: The Sixth Circuit Improperly Narrowed The Private Search Doctrine Of The Fourth Amendment In a Case of Child Pornography On A Digital Device*, 49 Creighton L. Rev. 177, 185 (2015).

The Court's decision in *Riley* was hailed by many in the media as a "sweeping victory for privacy rights in the digital age."[237] Commentators suggested that the Supreme Court had "entered the digital age and fundamentally changed how the Constitution protects our privacy."[238] Others remained cautiously optimistic that this decision signals that the Court is more prepared to engage in the challenges of the digital age ahead.[239] However, the decision has created a circuit split amongst lower courts, particularly related to the scope of the private search doctrine.[240]

When evaluating searches of electronic devices, Professor Orin Kerr explains that the application of the private search doctrine raises the following inquiry: "When a private party sees a file on a computer, what exactly has been searched for purposes of later reconstruction?"[241] Put another way, the scope of the private search doctrine governs "whether authorities can search an

---

237 *See* Adam Liptak, *Major Ruling Shields Privacy of Cellphone: Supreme Court Says Phones Can't Be Searched Without a Warrant*, The New York Times (June 25, 2014), http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html?_r=0.

238 *See* Stephen Vladeck, *How the Supreme Court Changed America This Year*, Politico Magazine (July 1, 2014), http://www.politico.com/magazine/story/2014/07/how-the-supreme-court-changed-america-this-year-108497

239 *See* Orin Kerr, *The Significance of Riley*, The Washington Post-The Volokh Conspiracy (June 25, 2014) (commenting that the Court's decision show how it would create very different results today in light of technological change and social practice); Marc Rotenberg and Alan Butler, *Symposium: In Riley v. California, a unanimous Supreme Court sets out Fourth Amendment for digital age*, SCOTUSblog (June 26, 2014), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/.

240 *Compare* United States v. Runyan, 275 F.3d 449 (5th Cir. 2001) (adopting single unit approach – defendant lost his expectation of privacy in entire disk when some of the files on it were viewed by a private party), *and* Rann v. Atchison, 689 F.3d 832 (7th Cir. 2012) (upholding search where police were substantially certain of the fact it contained child pornography and were free to search the entire device without a warrant), *with* United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015) (holding that police could not search a laptop without being virtually certain that the search would not exceed the earlier search by a private party), *and* United States v. Johnson, 806 F.3d 1323 (11th Cir. 2015) (adopting individual file approach and suppressing video evidence viewed by police that was not viewed during original search by private party).

241 Orin Kerr, *Sixth Circuit Creates Circuit Split On Private Search Doctrine For Computers*, The Washington Post-The Volokh Conspiracy (May 20, 2015) https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers/?utm_term=.35598bf86ddf.

entire collection of devices (e.g., CDs, USB or external hard drives) after a private party searched only a subset of the devices."[242] The answer, according to Professor Kerr, is dependent upon what the right "measuring unit" is.[243] Is it "the data, the file, the folder, the physical device, or something else?"[244] Prior to the Supreme Courts decision in *Riley*, the Fifth and Seventh Circuits adopted the single unit or physical device approach.[245] However, in post-*Riley* decisions, the Sixth and Eleventh Circuits have adopted a data or file level approach.[246] The following subsections analyze these different approaches, their underlying principles, and how they were impacted by the Court's decision in *Riley*.

A. Pre-*Riley*: Substantial Certainty And The Single Unit Approach[247]

In *United States v. Runyan*, the Fifth Circuit adopted the single unit approach.[248] In this case, defendant Robert Runyan became estranged from his wife, Judith, and subsequently filed for divorce.[249] In the months following their separation, Judith made several trips to Runyan's home

---

242 Pierre Grosdidier, *After Riley, Circuits Narrow Private Search Doctrine*, Law 360 (January 11, 2016) http://www.law360.com/articles/743564/after-riley-circuits-narrow-private-search-doctrine.

243 Orin Kerr, *Sixth Circuit Creates Circuit Split On Private Search Doctrine For Computers*, The Washington Post-The Volokh Conspiracy (May 20, 2015) (noting the unit the court chooses determines the outcome of the case)

244 Id.

245 *See infra* note 231.

246 Id.

247 Please note: he single unit and physical device approaches are functionally equivalent. The author has elected to adopt the single unit designation for the remainder of this paper.

248 United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001) (ruling that police do not exceed the scope of a prior private search when they examine particular items within a container that were not examined by the private searchers); *See* Orin S. Kerr, *Searches And Seizures In A Digital World*, Harvard Law Review, Vol. 119: 531, 555 (2005) (noting that *Runyan* offers an example of the physical device approach).

249 *Runyan*, 275 F.3d at 452.

to retrieve her personal property.[250] On one of these occasions, Judith found a desktop computer she claimed was hers.[251] Judith and her friend took the computer as well as a number of floppy disks, CDs, and ZIP disks that were on the desk and on the floor.[252] Later, Judith's friend viewed "approximately twenty of the CDS and floppy disks" and found they contained images of child pornography.[253] Judith and her friend turned the materials over to law enforcement.[254] The police subsequently reviewed the disks without obtaining a warrant and uncovered more evidence of child pornography.[255] Runyan was indicted on child pornography charges.[256]

Runyan filed a motion to suppress, arguing that the pre-warrant searches of the disks violated the Fourth Amendment.[257] The trial court denied the motion, finding that the pre-warrant police searches did not violate the Fourth Amendment because "the police did not exceed the scope of the private search conducted by Judith and her companions."[258] Runyan was then convicted and sentenced to 300 months in prison.[259] Runyan appealed, arguing in relevant part that the trial

---

250 Id.

251 *Id*. at 453.

252 Id.

253 Id.

254 Id.

255 *Id*. at 454-55.

256 *Id*. at 455.

257 Id.

258 Id.

259 Id.

court erred in "failing to suppress the evidence obtained directly and indirectly from the pre-warrant police searches."[260]

The Fifth Circuit initially stated that a defendant's expectation of privacy with respect to an unopened container is "persevered unless the defendant's expectation of privacy in the contents of the container has already been frustrated because the contents were rendered obvious by the private search."[261] The Fifth Circuit reasoned that this policy would prevent "fishing expeditions" and ensure that police officers are "substantially certain" of the contents before they open the container.[262] Accordingly, the court concluded that the police's pre-warrant examination of the disks *not viewed* by Judith or her friend "clearly exceeded the scope of the private search."[263] The court emphasized the lack of any identifying marks on the disks that would alert an ordinary viewer of their contents.[264] Additionally, it was not enough that the disks were found in the same location of Runyan's residence where other evidence of child pornography was found.[265] Therefore, the court concluded the police "exceeded the scope of the private search […] when they examined disks that the private searches did not examine."[266]

Despite the suppression of the unviewed disks, the court refused to accept Runyan's argument that the police also exceeded the scope of the private search because they examined more files on

---

260 Id.

261 *Id*. at 463-64.

262 *Id*. at 464.

263 Id.

264 Id.

265 Id.

266 Id.

the disks than the private searchers did.[267] Even though the record did not clearly indicate what files Judith and her friend initially viewed, the court did not suppress this evidence.[268]

The Fifth Circuit explained, in the context of a closed container search police do not exceed the private search when they examine more items within the closed container that the private individuals did not.[269] Accordingly, the *Runyan* court concluded, "police do not engage in a new 'search' for Fourth Amendment purposes each time they examine a particular item found within the container."[270] In this case, the container was the disk and the prior private search eliminated any expectation of privacy in the container.[271] Utilizing this approach, a more "detailed police search of the containers […] did not offend the Fourth Amendment.[272] Holding otherwise would "over-deter" law enforcement from "engaging in lawful investigation of containers where any reasonable expectation of privacy has already been eroded."[273]

The Seventh Circuit adopted *Runyan's* reasoning in *Rann v. Atchison*.[274] In this case, defendant Steven Rann was convicted of two counts of criminal sexual assault and one count of

---

267 Id.

268 *Id*. at 464-65.

269 *Id*. at 464.

270 *Id*. at 465.

271 Pierre Grosdidier, *After Riley, Circuits Narrow Private Search Doctrine*, Law 360 (January 11, 2016) http://www.law360.com/articles/743564/after-riley-circuits-narrow-private-search-doctrine.

272 Id.

273 Id.

274 Rann v. Atchison, 689 F.3d 832, 837 (7th Cir. 2012) (We find the Fifth Circuit's holding in *Runyan* to be persuasive, and we adopt it); *see also* Joel Varner, *Computers, the Private Search Doctrine, and the Fourth Amendment*, Michigan Telecommunications and Technology Law Review (last visited November 21, 2016) (noting same) http://mttlr.org/2015/11/05/computers-the-private-search-doctrine-and-the-fourth-amendment/.

child pornography.[275] The defendant's 15-year-old daughter, S.R., reported to law enforcement officials that he had sexually assaulted her.[276] S.R. also supplied the police with a digital camera memory card containing images of Rann sexually assaulting S.R.[277] Sometime later, S.R.'s mother brought police a computer zip drive that contained additional pornographic images of S.R. and her half-sister, K.G.[278] Rann did not move to suppress the images found on the zip drive and camera memory.[279] However, after being convicted Rann filed a habeas petition asserting that his trial counsel was ineffective for failing to move to suppresses the images recovered from the storage devices.[280] The Illinois Appellate Court denied the motion and Rann appealed.[281]

The 7th Circuit rejected Rann's argument that police exceeded the scope of the private search when it viewed additional items on the storage devices without first obtaining a warrant.[282]Applying the principles of *Runyan*, the 7th Circuit additionally stated that even if the police "more thoroughly" searched the digital storage devices the police search did not "exceed or expand" the scope of the initial private search.[283] The *Rann* court reasoned that this is because S.R. and her mother knew the contents of the storage devices and police were "substantially

---

275 *Id*. at 834.

276 Id.

277 Id.

278 Id.

279 Id.

280 *Id*. at 834-35.

281 Id.

282 *Id*. at 837.

283 Id.

certain" that the devices contained child pornography.[284] Accordingly, law enforcement was free to search the entire device without warrant and without violating the Fourth Amendment.[285]

B. Post-*Riley*: Narrowing The Scope Of The Private Search Doctrine And The File Level Approach

Since the Supreme Court's decision in *Riley*, the Sixth and Eleventh Circuits have adopted a "much narrower" scope for the private search doctrine as it applies to electronic devices.[286] First, in *United States v. Lichtenberger*, the United States Court of Appeals for the Sixth Circuit concluded that law enforcement violated the Fourth Amendment when it viewed the contents of the defendant's computer without a warrant.[287] In this case, defendant Lichtenberger and his girlfriend, Karley Holmes, lived together.[288] After Holmes learned that the defendant was previously convicted of child pornography offenses she had him removed from the shared home.[289] Later that day, Holmes retrieved the defendant's laptop with intention of searching it for

---

284 Id.

285 Pierre Grosdidier, *After Riley, Circuits Narrow Private Search Doctrine*, Law 360 (January 11, 2016) http://www.law360.com/articles/743564/after-riley-circuits-narrow-private-search-doctrine.

286 Id.; *see also* Joel Varner, *Computers, the Private Search Doctrine, and the Fourth Amendment*, Michigan Telecommunications and Technology Law Review (last visited November 21, 2016) (explaining that Unlike the Fifth and Seventh Circuits, the Sixth Circuit views a computer as a combination of multiple containers) http://mttlr.org/2015/11/05/computers-the-private-search-doctrine-and-the-fourth-amendment/.

287 *United States v. Lichtenberger*, 786 F.3d 478, 491 (6th Cir. 2015) (In light of the information available at the time the search was conducted, the strong privacy interests at stake, and the absence of a threat to government interests, we conclude that Officer Huston's warrantless review of Lichtenberger's laptop exceeded the scope of the private search Holmes had conducted earlier that day, and therefore violated Lichtenberger's Fourth Amendment rights to be free from an unreasonable search and seizure).

288 *Id*. at 480.

289 Id. (Holmes requested police remove him the home, which her mother owned. Police did so as Lichtenberger had an active warrant for failing to register as a sex offender.).

evidence of child pornography.[290] After hacking the password, Holmes "clicked on different folders" and eventually found thumbnail images of "adults engaging in sexual acts with minors."[291] After clicking through several of the images, Holmes closed the computer and contacted the police.[292]

Officer Huston responded to the call and asked Holmes to show him what he discovered.[293] Holmes proceeded to "open several folders" and "began clicking on random thumbnail images" to show the officer.[294] Officer Huston recognized the images as child pornography and asked Holmes to shut down the laptop.[295] Holmes later testified that she viewed approximately 100 images of child pornography saved in "several subfolders inside a folder entitled 'private'."[296] Additionally, she testified that she showed Officer Huston "a few pictures" from these files.[297] However, Holmes was "not sure" if they were among the original images she had seen in her original search.[298] Lichtenberger was indicted on child pornography charges.[299] The defendant filed a motion to suppress, arguing that "when Officer Huston directed Holmes to show him what

---

290 Id. (During the suppression hearing, Holmes explained that she was always suspicious about the laptop because the defendant would never let or use it or be near her when he used it).

291 Id.

292 Id.

293 Id.

294 Id.

295 *Id*. at 481.

296 Id.

297 Id.

298 Id.

299 Id.

she had found, [she] was acting as an agent of the government[,]" in violation of the Fourth Amendment.[300] Applying the Supreme Court's reasoning in *Riley,* the district court granted Lichtenberger's motion to suppress the laptop evidence.[301] The Government appealed.[302]

In upholding the district court's decision, the Sixth Circuit Court of Appeals first concluded that Holmes's initial search qualified as a private search.[303] However, the *Lichtenberger* Court found that the scope of Officer Huston's search exceeded that of Holmes' private search.[304] In reaching this conclusion, the court focused on the *Riley* Court's concerns[305] related to the immense storage capacity of digital devices and the implications such data has on privacy concerns.[306] It is because of these concerns that the court reasoned that Lichtenberger's laptop should be afforded the same level of protection as the cell phones in *Riley*.[307] Additionally, the court emphasized that the police could not be "virtually certain" that the subsequent search was

---

300 Id.

301 *Id*. at 487-88 (reaching the same conclusion as the *Riley* Court and holding that Lichtenberger's privacy interest, which is increased by the nature of information a laptop may reveal, outweighs the interest of the government).

302 *Id*. at 481.

303 *Id*. at 484-85 (applying the principles of *Jacobsen* to disagree with the lower court and finding a lack of agency relationship between the private actor and the government).

304 *Id*. at 485.

305 *Riley*, 134 S. Ct. 2473, 2489 (2014) (The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet).

306 *Id*. at 487-88 (stating that "under Riley, the nature of the electronic device greatly increases the potential privacy interests at stake, adding weight to one side of the scale while the other remains the same"); *see also* Emily Field, *Gov't Can't Use Warrantless Laptop Search, 6th Circ. Says*, Law360 (May 21, 2015) http://www.law360.com/articles/658936/gov-t-can-t-use-warrantless-laptop-search-6th-circ-says.

307 Id.

limited to the images Holmes previously viewed.[308] Even though the images viewed by law enforcement were evidence of child pornography they could have revealed any other amount of private information unrelated to the crime.[309] This lack of certainty was "dispositive" and supported the court's decision to uphold the district court's suppression of the evidence.[310]

The Eleventh Circuit adopted a similar approach in *United States v. Johnson*.[311] In this case, defendants Alan Johnson and Jennifer Sparks accidently left their cell phone at a Wal-Mart store.[312] Linda Vo, a Wal-Mart employee, found the phone and arranged to return it to the co-defendants.[313] However, before returning it Vo decided to look at the contents of the phone, which was not password-protected.[314] Upon doing so, Vo discovered images and videos of child pornography.[315]

Vo told her fiancé, David Widner, that she saw some "pretty weird" pictures involving a young girl.[316] Widner decided to view the images himself and scrolled through all of the

---

308 *Id*. at 488-89 (noting that there was no virtual certainty that the subsequent search would reveal other sensitive or private documents, not viewed during the private search).

309 *Id*. at 489 (Other documents, such as bank statements or personal communications, could also have been discovered among the photographs).

310 Id.

311 *United States v. Johnson*, 806 F.3d 1323 (11th Cir. 2015); *see* Sally Albertazzie, *Eleventh Circuit Limits Application of Private-Search Doctrine To Digital Data*, Lexology (January 16, 2016) http://www.lexology.com/library/detail.aspx?g=20dd32e3-c92f-4ebd-8737-10232fb379b2.

312 *Johnson*, 806 F.3d at 1329.

313 Id.

314 Id.

315 Id. (cell phone contained hundreds of images and videos of child pornography that were made using Spark's friend's four-year-old child).

316 *Id*. at 1330-31.

thumbnail images in the phone's photo album.[317] He also opened a few images to full size and watched one video.[318] After showing them to Vo, they contacted the police and turned over the phone.[319] Detective O'Reilly subsequently viewed the images on the phone, confirming they were in fact child pornography.[320] Detective O'Reilly opened all of the images to full size and viewed both the video that Widner had seen and another Widner had not.[321] Johnson and Sparks filed motions to suppress, which the district court denied.[322]

On appeal, the Eleventh Circuit held that Detective O'Reilly did not exceed the scope of the private search when he looked at photos – thumbnail and full-size images - or watched videos that Widner had viewed.[323] However, the court found that Detective O'Reily did exceed the scope of the private search when he watched the video Widner had not watched.[324] The court reasoned that allowing the second video to be admitted, "when no private party had first watched it" would run afoul of the Supreme Court's decision in *Riley*. As in *Lichtenberg*, the *Johnson* court focused on the Supreme Court's emphasis of data storage and privacy implications.[325] The court stated that a search of the cell phone may have "removed certain information from the

---

317 *Id*. at 1331.

318 Id.

319 Id.

320 *Id*. at 1331-32.

321 *Id*. at 1332.

322 *Id*. at 1333.

323 *Id*. at 1335.

324 *Id*. at 1336. (finding that the detective's review exceeded-not replicated-the breadth of the private search).

325 Id.

Fourth Amendment's protections," but not all of it.[326] Accordingly, the officer's viewing of the second video exceeded the scope of the private search and was suppressed.[327]

V. Conclusion

While this paper does not advocate for a particular approach, the author recognizes that there are strong proponents and critics on both sides.[328] In analyzing the current circuit split, the author hopes to have demonstrated the need for the Supreme Court to take action and settle the current split. This becomes clear when one recognizes that the only thing that distinguishes these factually similar fact patterns is the *Riley* decision.[329]

The Pre-*Riley* cases, *Runyan* and *Rann*, hold that a private search of one file in an electronic device opens the entire device up subsequent search by law enforcement. The Post-*Riley* cases, *Lichtenberger* and *Johnson*, mirror *Riley* and focus on the privacy implications associated with searching private data. Accordingly, these cases hold that a subsequent law enforcement search cannot exceed the specific files viewed. The Supreme Court's decision in *Riley* has impacted the application of the private search doctrine, even though it is not a

---

326 Id.

327 Id.

328 *Compare* Orin Kerr, *11th Circuit Deepens The Circuit Split On Applying The Private Search Doctrine To Computer*, The Washington Post-The Volokh Conspiracy (December 2, 2015) (advocating for a data-based approach adopted by the Sixth and Eleventh Circuits); *and* Stephen Labrecque, *"Virtual Certainty" In A Digital World: The Sixth Circuit's Application Of the Private Search Doctrine To Digital Storage Devices in United States v. Lichtenberger* 57 B.C.L. Rev. 177, 189 (2016) (arguing that the closed container approach to digital devices could result in significant violations of personal privacy and should not be adopted in future cases); *with* Katie Matejka, *Note: United States v. Lichtenberger: The Sixth Circuit Improperly Narrowed The Private Search Doctrine Of The Fourth Amendment In a Case of Child Pornography On A Digital Device*, 49 Creighton L. Rev. 177, 180 (2015) (criticizing the Sixth Circuit and arguing for the adoption of a closed container approach in child pornography cases).

329 Pierre Grosdidier, *After Riley, Circuits Narrow Private Search Doctrine*, Law 360 (January 11, 2016) http://www.law360.com/articles/743564/after-riley-circuits-narrow-private-search-doctrine.

private search case. Accordingly, the Supreme Court should settle the current circuit split and clarify the contours of Fourth Amendment in the digital world.